LISTING OF CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application:

1. (Currently Amended) A method of providing devices that generate digital signatures such that each device may be reliably and uniquely identified by a third party that receives an electronic message generated by a device and utilizes the electronic message for a message authentication, comprising the steps of:

a. manufacturing in a secure environment a device that generates a digital signature utilizing a private key of a public-private key pair;

b. creating a public-private key pair in the device while the device is still within the secure environment, the private key for utilization in generating a digital signature for an electronic message, the public key exportable for use by third parties in connection with authenticating the electronic message;

c. storing the private key within the device utilizing security features to safeguard the private key against divulgement thereof by the device;

d. securely linking the public key with other information, the other information including the security features, by storing the public key and the other information in a database within the secure environment; and

e. releasing the device from the secure environment for use in connection with generating a digitally signed electronic message that is provided by a user of the device to a third party; ~~that receives and authenticates the electronic message based on the public key and the other information.~~

whereby the other information and security features securely linked with the public key and stored in the database within the secure environment are used by the third party to authenticate the electronic message received by the third party.

2. (Original) The method of claim 1, wherein each private-public key pair is created within each device based on a random number produced by a random number generator disposed within each device.

3. (Original) The method of claim 2, wherein each digital signature generated by each device is a random number.

4. (Previously Presented) The method of claim 1, wherein the other information comprises respective security features and a manufacturing history of each device.

5. (Previously Presented) The method of claim 1, further comprising the step of identifying a particular manufactured device by authenticating a message using one of a plurality of public keys in the database within the secure environment, a digital signature for the message having been generated by the particular manufactured device.

6–20. (Cancelled)

21. (Currently Amended) The method of claim 1, wherein the public key and the other information linked therewith is obtained by the third party from a Secure Entity.

22. (Previously Presented) The method of claim 1, wherein the other information stored in the database includes the identity of a plurality of third-parties with which an account is maintained, the accounts being identified by one of a plurality of third-party account identifiers.

23. (Currently Amended) The method of claim 22, wherein the public key, [[and]] the other information, and the security features are [[is]] indexed in the database by unique account identifiers such that the public key, [[and]] the other information, and the security features for a user [[is]] are retrievable from the database based on the account identifier.

24. (Previously Presented) The method of claim 23, wherein the public key is the unique account identifier.

25. (Currently Amended) The method of claim 1, wherein the public key, [[and]] the other information, and the security features stored in the database for each user further includes user-specific information.

26. (Previously Presented) The method of claim 25, wherein the user-specific information includes the name and address of the user.

27. (Currently Amended) The method of claim 1, further comprising the step of establishing an account on behalf of a user of a device with a third-party by communicating the public key of the device, [[and]] the other information, and the security features linked with the public key from the database to the third-party.

28. (Currently Amended) The method of claim 1, wherein the public key of the device, [[and]] the other information, and the security features linked with the public key are [[is]] communicated to a third party upon the request of the third-party.

29. (Currently Amended) The method of claim 1 further comprising the step of updating the public key of a user maintained with at least two independent third-parties with a new public key of the user, comprising the steps of:

a. receiving an EC, the EC including an account identifier and a message including the new public key and a digital signature therefore; [[,]]

b. authenticating the message of the EC using the public key associated with the account in the database identified by the account identifier, and upon successful authentication thereof; and [[,]]

c. sending an EC to each of the third-parties, each EC including the new public key and the third-party account identifier for the respective third-party maintained in the database and associated with the account identified by the account identifier.

30. (Previously Presented) The method of claim 29, further comprising the step of digitally signing a message involving the new public key of the user and a third-party account identifier.

31. (Previously Presented) The method of claim 29, further comprising the step of sending the EC received from the user to each of the third-parties.

32. (Currently Amended) The method of claim 1, wherein the security features are selected from the group including but not limited to: electronic shielding, zeroization, auditing, tamper evidence, authentication capabilities, and/or tamper response.

33. (New) The method of claim 32, wherein the authentication capabilities include use of an initialization PIN by the user of the device before the device may be used.

34. (New) The method of claim 33, wherein the authentication capabilities include use of a personalization PIN by the user of the device each time the device is used.